IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UBIQUITI NETWORKS, INC., *Plaintiff,* v. CAMBIUM NETWORKS, INC.; CAMBIUM NETWORKS, LTD.; BLIP NETWORKS, LLC; WINNCOM TECHNOLOGIES, INC.; SAKID AHMED; and DMITRY MOISEEV. *Defendants*.	Civil Action No.: 1:18-cv-05369 **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Ubiquiti Networks, Inc. ("Plaintiff" or "Ubiquiti") brings this action against Defendants Cambium Networks, Inc. ("Cambium"), Cambium Networks, Ltd. ("Cambium Networks"), Blip Networks, LLC ("Blip"), Winncom Technologies, Inc. ("Winncom"), Sakid Ahmed, and Dmitry Moiseev and hereby alleges as follows:

NATURE OF THE ACTION

1. This is a Complaint for injunctive relief and damages based on Cambium's intentional, commercially motivated, unauthorized access, reverse engineering and hacking of Ubiquiti's M-series wireless devices and trafficking in hacked firmware that deletes, modifies, and makes unauthorized copies of portions of the Ubiquiti firmware on the Ubiquiti M-series devices, eliminates Ubiquiti copyright notices to conceal Cambium's infringement, eliminates firmware restrictions Ubiquiti put in place to ensure operation in conformity with Federal Communications Commission ("FCC") requirements and licenses, and circumvents access control measures on the

Ubiquiti M-series devices, all in violation of the Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act ("DMCA"), the Illinois Computer Crime Prevention Law, the Copyright Act, various state laws and the Ubiquiti firmware license agreements. Cambium's promotion and distribution of the hacked firmware as a product called Elevate (the "Hacked Firmware") is based on flagrant misrepresentations and false advertising in violation of the Lanham Act and state competition laws, and tortiously interferes with Ubiquiti's license agreements with Ubiquiti customers and Ubiquiti's prospective customers and business relationships. Once hacked with the Hacked Firmware, Ubiquiti M-series devices thereafter violate FCC rules and regulations and FCC licenses for the equipment.

2. The sale and marketing of the Hacked Firmware was carried out through an elaborate scheme of mail and wire fraud involving material misrepresentations and omissions regarding the nature of the Hacked Firmware, willful copyright infringement, and misappropriation of Ubiquiti's time, money, brand recognition, and good will established with existing and prospective customers. Cambium, Cambium Networks, Sakid Ahmed—Vice President of Engineering at Cambium Networks, Dmitry Moiseev—Project Engineer at Cambium Networks, and Winncom (collectively, the "Hacking Enterprise") conspired together and with co-conspirator Blip to defraud Ubiquiti customers and ensure financial gain in connection with marketing, sale, distribution, and use of the Hacked Firmware.

PARTIES

3. Plaintiff Ubiquiti is a corporation organized under the laws of the State of Delaware, with its principal place of business at 685 Third Avenue, 27th Floor, New York, New York 10017.

4. Defendant Cambium is a corporation organized under the laws of the State of Delaware, with its principal place of business at 3800 Golf Road, Suite 360, Rolling Meadows, Illinois 60008.

5. Defendant Cambium Networks is a British limited liability company with its principal place of business in England. Cambium Networks is the parent company of Cambium.

6. Defendant Blip is an Illinois limited liability company, with its principal place of business at 6 Sharp Rock Road, Ava, Illinois 62907-2528.

7. Defendant Winncom is an Ohio corporation, with its principal place of business at 28900 Fountain Parkway # B, Solon, Ohio 44139-4383.

8. Defendant Sakid Ahmed is the Vice President of Engineering at Cambium Networks and a resident of Chicago, Illinois.

9. Defendant Dmitry Moiseev is a Project Engineer at Cambium Networks and a resident of Hoffman Estates, Illinois.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Ubiquiti's claims arising under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, the claims arising under the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 *et seq.* ("RICO"), the Lanham Act, 15 U.S.C. § 1125 *et seq.*, and the Copyright Act, 17 U.S.C. § 101 *et seq.* pursuant to this Court's federal question jurisdiction under 28 U.S.C. § 1331. This Court also has supplemental jurisdiction over all other claims asserted herein pursuant to 28 U.S.C. § 1367 because those claims are so related to the claims brought under the federal statutes so as to form part of the same case or controversy.

11. This Court has personal jurisdiction over Defendant Cambium. Cambium is registered to do business in the State of Illinois and has a regular and established place of business

in Illinois and this District at 3800 Golf Road, Suite 360, Rolling Meadows, Illinois 60008, and is and has been doing business in Illinois and this District at all times relevant hereto.

12. This Court has personal jurisdiction over Defendants Sakid Ahmed and Dmitry Moiseev, Illinois residents who live, work, are employed, and carried out acts described herein within the Northern District of Illinois.

13. This Court has personal jurisdiction over Defendants because directly or through intermediaries, they have committed acts within or directed at Illinois, causing harm herein and giving rise to this action, and/or have established minimum contacts with Illinois such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

14. Venue is proper in this Court because Defendants Cambium, Ahmed, Moiseev, and Blip reside or may be found in this District. *See* 28 U.S.C. §§ 1391(b) & (c).

15. Venue is also proper because a substantial part of the events and omissions giving rise to the instant action occurred within this District. Unlawful and improper conduct including the violations of the CFAA, copyright infringement, and fraudulent mailing and interstate wire communications have occurred and originated within this District.

16. Venue is also proper pursuant to 18 U.S.C. § 1965 and 28 U.S.C. § 1391 because Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

Ubiquiti and Its Products

17. Founded in June 2005, Ubiquiti is a next generation communications technology company that designs and develops, among other things, proprietary wireless networking technologies. Ubiquiti's products and solutions have bridged the digital divide between rural and urban markets by fundamentally changing the economics of deploying high performance networking solutions in underserved and underpenetrated markets globally. Ubiquiti's technology

platforms focus on delivering industry-leading performance, compelling price-performing characteristics and an unparalleled user experience. Ubiquiti has reduced high product and network deployment costs and other business model inefficiencies to enable rapid market adoption of its products and solutions in rural and emerging markets.

18. Ubiquiti has expended considerable time and resources to advertise and promote its products and brand throughout the world. In addition to traditional advertising, Ubiquiti hosts a Ubiquiti Network Community Forum for users of Ubiquiti products who spread information about the products by word of mouth.

19. Over the last eight years, Ubiquiti has spent over 500 million dollars investing in its proprietary products, developing its distribution network, and creating goodwill in the marketplace.

20. Ubiquiti has received substantial unsolicited accolades and press for its successful broadband product line. In 2007, Ubiquiti received significant attention when a group of Italian amateur radio operators set a distance world record for point-to-point links in the 5.8 GHz spectrum using Ubiquiti cards and antennas. Ubiquiti received the Wireless Internet Service Providers Association ("WISPA") Manufacturer of the Year awards in 2010, 2011, 2014, and 2016.

Ubiquiti M-Series Devices

21. Ubiquiti's extensive broadband product line includes Ubiquiti's M-series devices: the NanoStation M, NanoStation Loco M (collectively, "NanoStations"), which are wireless "customer premises equipment" that permit outdoor throughput; the NanoBridge M-series, the NanoBeam M-series and the PowerBeam M-series, which are all wireless bridges that wirelessly rebroadcast packets received; and the AirGrid M-series and the Rocket M-series. The AirGrid M is a broadband wireless device that combines antenna and radio using Ubiquiti's proprietary

Innerfeed technology. The Rocket M is a radio device with enhanced receivers that delivers broadband connectivity through interchangeable antennas.

22. Ubiquiti launched AirMAX® and its M-series product line in 2009. AirMAX incorporates proprietary radio frequency (RF) technology, antenna design, and firmware, which simplify adoption and use of base stations, back haul equipment, and customer premises equipment (CPE).

Ubiquiti M-Series Device Firmware

23. All Ubiquiti AirMAX® products run on Ubiquiti's proprietary airOS® operating system embodied in Ubiquiti's firmware, and under Ubiquiti's proprietary AirMAX® protocol. The AirMAX® logo is present on the packaging of all Ubiquiti AirMAX® products. The airOS® logo appears on screen when a user logs in to the web interface for Ubiquiti M-series devices using the Ubiquiti username and password.

24. The user interface for a M-series device provides a path for upgrading the device firmware. The Ubiquiti user interface is accessed at a designated IP address using a web browser. On the first access to the user interface, the Ubiquiti customer is presented with the "Terms of Use" and the "Ubiquiti Firmware User License Agreement."

25. The unsigned versions of the Ubiquiti firmware include checks for determining whether a firmware upgrade is compatible. Firmware that does not pass the checks is rejected and not installed.

26. Ubiquiti introduced a "signed" version of the airOS® firmware for M-series devices in 2017, including airOS firmware versions 5.6.15 and 6.0.3. The signed versions also allow upgrading, but a more robust signature verification performed by the boot loader verifies new firmware. Users may upgrade with a newer version of Ubiquiti firmware by downloading and installing the newer version.

Ubiquiti Product Packaging, Labeling, and Branding

27. All Ubiquiti AirMAX® product packaging for M-series devices is labeled with Ubiquiti's name and corporate address, Ubiquiti's domain name (www.ubnt.com), the UBIQUITI® trademark and Ubiquiti logo, and the AirMAX® trademark. Each Ubiquiti M-series product is also branded with a trademark associated with that M-series device.

28. Ubiquiti owns registered trademarks used in branding the Ubiquiti M-series products, including: UBIQUITI® - Reg. No. 4,524,111; NANOSTATION® - Reg. No. 4,323,172; NANOBRIDGE® - Reg. No. 4,319,934; NANOBEAM® - Reg. No. 4,519,296; ROCKET® - Reg. No. 4558,159.

29. Ubiquiti owns common law trademarks in other marks used to brand Ubiquiti M-series devices.

30. Ubiquiti owns U.S. Copyright No. TXu001795146 for Ubiquiti firmware airOS version 5.2.1 and U.S. Copyright No. TXu001795146 for Ubiquiti firmware airOS version 5.3. *See* Exhibit A.

31. Ubiquiti also marks products with a unique identifying code called a Media Access Control ID ("MAC ID"). The product packaging and the product labels also contain a unique FCC Identification number approved by the FCC, SWX-M2, which can be used to find information about the manufacturer and the product, including approved frequency ranges, via the FCC website. The packaging and the labels also have the European Union "CE" mark, certifying compliance with European Union safety, health, and environmental protection requirements.

32. In general, Ubiquiti designs and develops each of its products in-house, and uses contract manufacturers to manufacture the products according to Ubiquiti's proprietary designs. Ubiquiti has stringent standards that contract manufacturers are required to meet, and closely

monitors the quality of products that they produce to assure that they meet Ubiquiti's high quality standards.

33. Consumers have come to associate the Ubiquiti brand with its high quality standards and cutting-edge technologies. This is the result of Ubiquiti's extensive investment of time, money, and resources into establishing consumer goodwill and brand recognition.

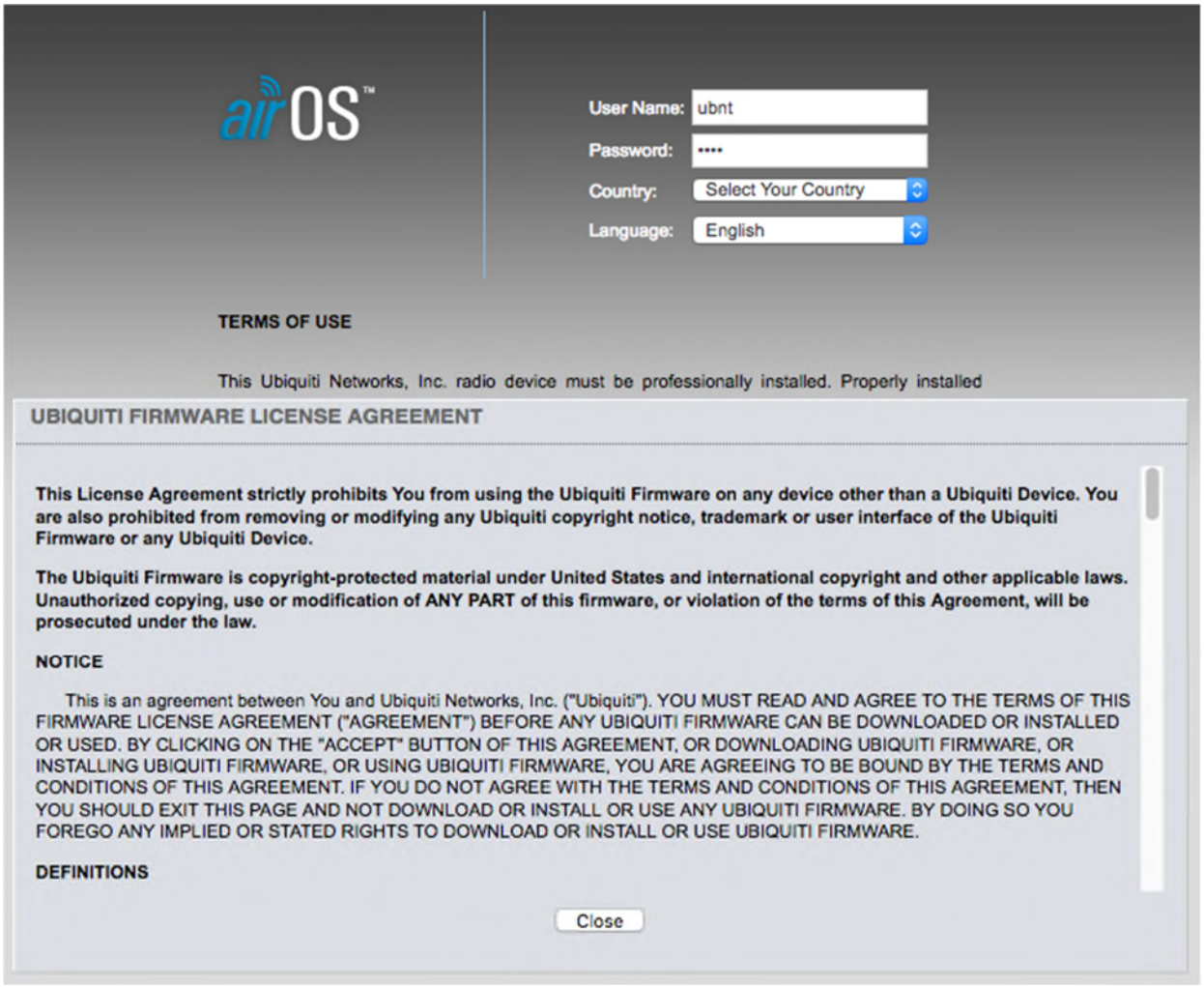
34. Ubiquiti uses a worldwide network of distributors to market and distribute its products. Ubiquiti's products are currently offered in the United States and in over 65 other countries.

35. Ubiquiti primarily sells its M-series devices to wireless Internet service providers (WISPs). WISPs purchase and deploy Ubiquiti M-series products and Ubiquiti access points with which the Ubiquiti M-series products communicate over medium to long range distances to build out wireless broadband networks that span wide geographic areas.

36. The Ubiquiti M-series devices are designed to be affixed by a WISP to structures, such as a building, to establish fixed wireless networks. The Ubiquiti AirMAX® radio protocol is used for wireless communications between Ubiquiti devices.

The Ubiquiti Firmware License Agreements For Its M-Series Products

37. Ubiquiti M-series devices include a user interface for Ubiquiti customers to configure Ubiquiti M-series devices. The user interface is accessed at a designated IP address using a web browser. On the first access, the Ubiquiti customer is presented with the "Terms of Use" and the "Ubiquiti Firmware User License Agreement" as shown below:



The Ubiquiti customer is required to agree to both the Terms of Use and the Ubiquiti Firmware License Agreement, via a checkbox. *See* Terms of Use and the Ubiquiti Firmware License Agreement (Exhibit B).

38. The Ubiquiti Firmware License Agreement requires users to agree to its terms prior to using Ubiquiti firmware and provides in pertinent part:

> This License Agreement strictly prohibits You from using the Ubiquiti Firmware on any device other than a Ubiquiti Device. You are also prohibited from removing or modifying any Ubiquiti copyright notice, trademark or user interface of the Ubiquiti Firmware or any Ubiquiti Device.
>
> The Ubiquiti Firmware is copyright-protected material under United States and international copyright and other applicable

> laws. Unauthorized copying, use or modification of ANY PART of this firmware, or violation of the terms of this Agreement, will be prosecuted under the law.
>
> NOTICE
> This is an agreement between You and Ubiquiti Networks, Inc. ("Ubiquiti"). YOU MUST READ AND AGREE TO THE TERMS OF THIS FIRMWARE LICENSE AGREEMENT ("AGREEMENT") BEFORE ANY UBIQUITI FIRMWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE "ACCEPT" BUTTON OF THIS AGREEMENT, OR DOWNLOADING UBIQUITI FIRMWARE, OR INSTALLING UBIQUITI FIRMWARE, OR USING UBIQUITI FIRMWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND NOT DOWNLOAD OR INSTALL OR USE ANY UBIQUITI FIRMWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE UBIQUITI FIRMWARE.

39. The Ubiquiti Firmware License Agreement prohibits, among other things: copying, modifying or reverse engineering the firmware; removing or modifying copyright notices or user interfaces on Ubiquiti devices; and circumventing any software protection mechanisms, including any mechanism used to restrict or control the functionality of the Ubiquiti firmware. The Ubiquiti Firmware License Agreement provides in pertinent part:

> a. **You may not, and shall not permit others to: . . .**
>
> e. copy the Ubiquiti Firmware (except as expressly permitted above), or copy the accompanying documentation;
>
> f. modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Ubiquiti Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Ubiquiti Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or

> g. distribute, rent, transfer or grant any rights in the Ubiquiti Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Ubiquiti;
>
> h. remove any Ubiquiti copyright notice or Ubiquiti branding from the Ubiquiti Firmware or modify any user interface of the Ubiquiti Firmware or Ubiquiti Device.

40. The Ubiquiti Firmware License Agreement provides for automatic termination in the event that the user violates the Firmware License Agreement, stating in pertinent part:

> Unauthorized copying of the Ubiquiti Firmware or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make available to Ubiquiti other legal remedies. . . . Upon termination of this license for any reason You will destroy all copies of the Ubiquiti Firmware. Any use of the Ubiquiti Firmware after termination is unlawful.

41. Ubiquiti allows its customers to download Ubiquiti firmware updates for use on Ubiquiti M-series devices from the Ubiquiti website, by first agreeing to the terms of an End User License Agreement (EULA). *See* EULA (Exhibit C).

42. The EULA applicable to any Ubiquiti firmware downloaded from the Ubiquiti website, like the Firmware License Agreement, also prohibits removing or modifying copyright notices or user interfaces on Ubiquiti devices, and prohibits unauthorized copying, modification or removal of any part of the Ubiquiti firmware. The EULA also prohibits reverse engineering and circumventing any software protection mechanisms, including any mechanism used to restrict or control the functionality of the Ubiquiti firmware. Violations of the EULA result in automatic termination of the EULA. Ubiquiti's Terms of Use, Firmware License Agreement, and EULA applicable to Ubiquiti firmware are collectively referred to as Ubiquiti's "Firmware License Agreements."

Cambium's Creation of Hacked Firmware Targeting Ubiquiti M-Series Devices, Hacking, Unlawful Conduct, and Fraud

43. On information and belief, prior to November 30, 2016, Cambium acquired one or more Ubiquiti M-series wireless devices and at least one version of Ubiquiti's Air/OS firmware for the unauthorized purposes of reverse engineering the Ubiquiti firmware for M-series devices, accessing proprietary Ubiquiti information embedded in the firmware, copying portions of the firmware, modifying the firmware and user interfaces and developing and trafficking in Hacked Firmware targeting Ubiquiti M-series devices, and capitalizing on Ubiquiti's product development investment and customer goodwill. The Hacked Firmware does all of the following without authorization and in violation of Ubiquiti firmware license agreements:

44. The Hacked Firmware deletes portions of the Ubiquiti firmware and Ubiquiti user interfaces from Ubiquiti M-series devices.

45. The Hacked Firmware selectively modifies and copies portions of Ubiquiti firmware.

46. The Hacked Firmware makes unauthorized access to portions of the firmware that remain on Ubiquiti M-series devices after the hack.

47. The Hacked Firmware replaces the original radio software on Ubiquiti M-series devices with different, unauthorized radio software that causes the devices to stop operating in conformity with FCC requirements and equipment authorizations.

48. The Hacked Firmware circumvents access control measures on M-series devices.

49. On information and belief, Cambium reverse engineered the Ubiquiti firmware stored on M-series devices, in order to study the structure and proprietary aspects of the Ubiquiti firmware to create Hacked Firmware capable of circumventing Ubiquiti's access control mechanisms, including mechanisms used to verify firmware as permissible on M-series devices.

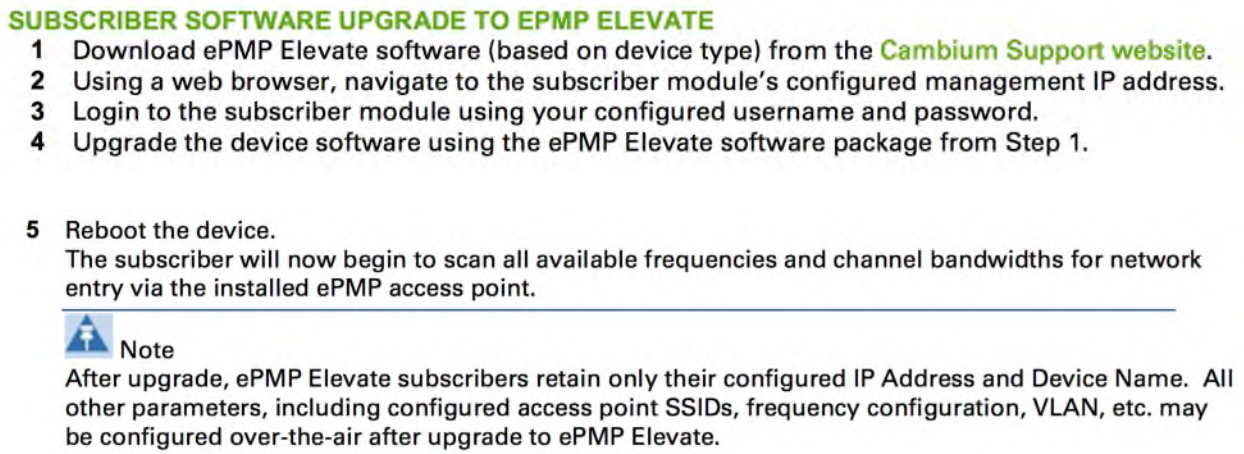
50. The Hacked Firmware removes proprietary Ubiquiti notices on Ubiquiti M-series devices.

51. The Hacked Firmware changes the user interfaces for M-series devices and makes unauthorized use of Ubiquiti trademarks in the user interfaces.

52. The Hacked Firmware renders the Ubiquiti M-series devices incapable of communicating with other Ubiquiti access points using Ubiquiti's radio software and instead causes the hacked Ubiquiti M-series devices only to communicate with Cambium access points.

53. Cambium instructs Ubiquiti licensees and customers to download the Hacked Firmware, open the Ubiquiti user interface on Ubiquiti M-series devices used for configuration, and to install the Hacked Firmware on M-series devices in violation of Ubiquiti firmware license agreements.

54. Cambium directs Ubiquiti's licensees using Ubiquiti M-series products to install the Hacked Firmware on Ubiquiti M-series products by following the ePMP Elevate Quick Start Guide (Exhibit D), excerpted below, as well as by following an online video:



SUBSCRIBER SOFTWARE UPGRADE TO EPMP ELEVATE

1 Download ePMP Elevate software (based on device type) from the Cambium Support website.
2 Using a web browser, navigate to the subscriber module's configured management IP address.
3 Login to the subscriber module using your configured username and password.
4 Upgrade the device software using the ePMP Elevate software package from Step 1.

5 Reboot the device.
The subscriber will now begin to scan all available frequencies and channel bandwidths for network entry via the installed ePMP access point.

Note
After upgrade, ePMP Elevate subscribers retain only their configured IP Address and Device Name. All other parameters, including configured access point SSIDs, frequency configuration, VLAN, etc. may be configured over-the-air after upgrade to ePMP Elevate.

Figure 1 – Elevate firmware update instructions from ePMP Elevate Quick Start Guide v3.2 (p. 5) (Ex. D)

55. Cambium formats the Hacked Firmware to be accepted by Ubiquiti's firmware update process and to hack M-series devices and the installed firmware in violation of Ubiquiti's Firmware License Agreements. Incorrectly formatted firmware is rejected by the Ubiquiti firmware.

56. After a Ubiquiti M-series device is hacked with the Hacked Firmware, the device's entire Ubiquiti user interface is replaced with a Cambium User Interface. This violates the Ubiquiti Firmware License Agreement.

57. Most Ubiquiti trademarks and logos are removed in the hacked User Interface However, Cambium still uses the M-series device trademarks, such as NANOSTATION®, within the hacked User Interface when a NanoStation M5 device has been taken over by the Hacked Firmware.

58. Each page of the Ubiquiti User Interface contains a Ubiquiti copyright notice. Cambium's replacement User Interface removes these notices and instead contains only Cambium Networks copyright notices. The removal of the Ubiquiti copyright notice is a violation of the Ubiquiti Firmware License Agreements.

59. Cambium's installation of the Hacked Firmware on Ubiquiti M-series devices, and such installation on M-series devices by others at Cambium's urging, is a violation of FCC rules.

60. Installation of the Hacked Firmware on Ubiquiti M-series devices modifies the Ubiquiti firmware and causes the Ubiquiti M-series devices to transmit with characteristics that are not allowed by the FCC equipment authorization and FCC rules, or the original Ubiquiti firmware, in violation of the Ubiquiti Firmware License Agreement.

61. Cambium admits that its firmware exceeds the original transmission thresholds:

Known problems or limitations (System Release 3.4)

Tracking Description / Workaround

. . .

14458 [ePMP Elevate 2.4, XM] Cambium Elevate operating Tx Power exceeds original nonCambium software-configured Tx Power by 1.5 – 3 dBm"

See Cambium Release Notes v. 3.5.1 (Exhibit E)

Cambium's Unlawful Promotion and Distribution of Hacked Firmware

62. In selling the Hacked Firmware, Cambium misleads and induces customers to make two significant modifications to two separate Ubiquiti products: (1) the Ubiquiti Firmware and (2) the Ubiquiti M-Series devices. *See generally* Exhibit F (Transcription of Portions of November 30, 2016 ePMP Elevate Webinar).

63. Cambium describes the Hacked Firmware, which it refers to as ePMP Elevate, as "an innovative software solution" that allows customers to "increase performance ***without replacing installed hardware***." (Exhibit G) (emphasis added), https://www.cambiumnetworks.com/products/access/epmp-elevate/.

64. According to Cambium, the ePMP Elevate software is intended to allow fixed wireless broadband networks to gain capabilities of the Cambium Networks' ePMP platform including frequency reuse enabled by GPS Synchronization and Smart Beamforming.

65. As a commercial benefit and cost savings, Cambium promotes the Hacked Firmware as a means to use the existing infrastructure licensed by other companies. The ePMP™ Elevate software product is designed to be used "even on non-Cambium Networks 802.11n-based hardware." (Exhibit H). According to Cambium, "Saving the cost and time of a total network replacement, an operator simply installs an ePMP Access Point and loads ePMP Elevate software onto their deployed subscriber modules." (Ex. G).

66. As material omissions, Cambium fails to tell customers that the use of the Hacked Firmware makes modifications to M-series devices and Ubiquiti firmware that violates Ubiquiti

firmware license agreements, violates FCC requirements and rules, and violates Ubiquiti's intellectual property rights.

67. The Ubiquiti Firmware is modified—portions remain, portions are modified, portions are removed and portions are copied—when the Cambium Hacked Firmware is installed.

68. Cambium officials highlight that the Hacked Firmware modifies the Ubiquiti M-series devices and firmware, and they promote the modification as a commercial benefit. For example, in the ePMP Portfolio Overview (Exhibit I), Cambium's promotional literature notes that the ePMP Elevate software product can "leverage an existing 802.11-based installed network and add synchronization without the cost of replacing the entire network." (Ex. I, Page 7). The Ubiquiti® XW/XM (including the trademark) is also listed as a supported product. (*Id.*).

69. Exhibit J shows a comparison between the user interface for the Ubiquiti PowerBeam M series product taken from the AirOS user guide and the user interface for an "Elevated" Ubiquiti product. The Ubiquiti user interface has a copyright notice on the bottom and features "Genuine Product" along with trademarks for the product name, AirOS and a design. The Cambium user interface eliminates the Ubiquiti copyright notice and replaces it with a Cambium copyright notice. It also makes unauthorized use of the Ubiquiti product name, in this instance the NanoBeam M5.

70. On or about November 30, 2016, Cambium began publicly promoting the Hacked Firmware under the name "Elevate" and "ePMP Elevate" for large scale distribution through a webinar, its website, and other avenues.

71. Cambium has continued to heavily promote the Hacked Firmware in the United States and throughout the world with additional webinars directed at WISPs, and marketing and distribution of literature and web pages through third party distributors, including distributors used

by both Cambium and Ubiquiti. Cambium has marketed the Hacked Firmware at industry conferences attended by WISPs, Cambium, and Ubiquiti and through live educational seminars directed at distributors and WISPs and demonstrating hacking Ubiquiti M-series devices using the Hacked Firmware.

Summary of Cambium's Illicit Conduct

72. Cambium's development, promotion and distribution of the Hacked Firmware violates the Ubiquiti Firmware License Agreements. Through Cambium's widespread promotion and distribution of the Hacked Firmware, Cambium willfully, and with full knowledge of Ubiquiti's proprietary rights, induces third parties, including Ubiquiti customers, to violate the Ubiquiti Firmware License Agreements and to violate Ubiquiti's copyrights and misappropriate Ubiquiti's proprietary information embedded in the firmware by installing and using Hacked Firmware on Ubiquiti M-series devices.

73. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, makes unauthorized copies of and modifies the configuration portion of Ubiquiti's firmware present on Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

74. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes the Ubiquiti kernel, including Ubiquiti radio control software, and the AIRMAX® technology platform on Ubiquiti M-series devices, in violation of the Ubiquiti Firmware License Agreements.

75. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes the Ubiquiti file system software on Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

76. As described herein, the Hacked Firmware preserves other portions of the Ubiquiti firmware present on M-series devices and makes unauthorized use of the Ubiquiti firmware after the Hacked Firmware is installed and running on Ubiquiti M-series devices.

77. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, preserves and makes unauthorized use of Ubiquiti's binary, proprietary calibration portion of the firmware present on the Ubiquiti M-series devices in violation of the Ubiquiti Firmware License Agreements.

78. As described herein, the Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, deletes and replaces the user interfaces on Ubiquiti M-series devices with a completely different, hacked user interface in violation of the Ubiquiti Firmware License Agreements.

79. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device eliminates all Ubiquiti copyright notices from the user interface on M-series devices, in violation of the Ubiquiti Firmware License Agreements.

80. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device replaces Ubiquiti copyright notices in a hacked user interface on M-series devices with Cambium copyright notices, notwithstanding the presence of Ubiquiti firmware on the hacked device.

81. The Hacked Firmware when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device includes Ubiquiti trademarks in the hacked user interface.

82. The Hacked Firmware, when installed by Cambium, a Cambium distributor or a Ubiquiti customer on a Ubiquiti M-series device, completely replaces the radio software and

thereafter permits the entry of radio transmission values through the hacked user interface that exceed radio restrictions implemented on the M-series devices and defeats Ubiquiti radio controls all in violation of the Ubiquiti Firmware License Agreement and FCC Rules and Regulations.

83. Cambium intentionally misleads and induces distributors and Ubiquiti customers to willfully and intentionally breach Ubiquiti's copyrights in its firmware by making unauthorized copies of copyrighted portions of Ubiquiti's firmware and by copying, installing or re-installing copies Ubiquiti's copyrighted firmware on M-series devices without authorization for the sole purpose of facilitating the hacking of Ubiquiti M-series devices by installing or reinstalling the Hacked Firmware.

84. Cambium's Hacked Firmware is a product of unauthorized reverse engineering of the Ubiquiti firmware stored on M-series devices and incorporates features capable of circumventing Ubiquiti's access control mechanisms, including mechanisms used to verify firmware as permissible on M-series devices.

85. The Hacked Firmware includes replacement radio software that changes the radio of M-series devices such that operation of the modified devices is impermissible under the FCC's Rules and Regulations.

86. Cambium traffics in Hacked Firmware that it directs distributors and Ubiquiti customers to install on Ubiquiti M-series devices to circumvent the access control protection mechanisms of the Ubiquiti firmware. This allows the Hacked Firmware to copy and gain unauthorized access to proprietary calibration and configuration information preserved on the M-series devices after the hacking.

87. Cambium's Hacked Firmware thereafter changes the radio on Ubiquiti M-series devices and causes the Ubiquiti M-series devices to transmit at power levels and with frequencies that violate FCC rules and equipment authorizations.

88. In early 2017, Ubiquiti introduced "signed" versions of the Ubiquiti AirOS firmware on newly produced M-series devices, and made these signed versions available for download for M-series devices, including AirOS firmware versions 5.6.15 and 6.0.3. These firmware versions are more difficult to hack than prior versions. Yet, Cambium has provided its end users with instructions on ways to attempt to hack the signed AirOS firmware versions.

89. Cambium traffics in Hacked Firmware and instructions to Ubiquiti customers that circumvent additional access controls on signed versions of Ubiquiti firmware for M-series devices. Cambium's instructions are premised on intentional, unauthorized copying of copyrighted Ubiquiti firmware in order to defeat the signed versions of Ubiquiti firmware for M-series devices, followed by additional hacking of the Ubiquiti M-series devices with the Hacked Firmware to circumvent access control mechanisms within the Ubiquiti firmware, and copy and gain unauthorized access to proprietary calibration and configuration information preserved on the M-series devices after the hacking.

90. Cambium's promotion of and trafficking in Hacked firmware is willful, wanton, fraudulent, and has been deliberately designed and carried out to damage Ubiquiti's customer relationships, unfairly compete with Ubiquiti and migrate Ubiquiti customers to Cambium customers.

91. Cambium and those distributors, customers and other agents that Cambium has misled and induced to commit willful breaches and violations of the Ubiquiti Firmware License Agreements described herein each exceeded the limited, authorized access that Ubiquiti provides

to use the firmware on Ubiquiti M-series devices. As a result, Cambium and/or its agents hacking of the Ubiquiti firmware in Ubiquiti M-series devices in furtherance of creating the Hacked Firmware immediately and automatically terminated the Ubiquiti Firmware License Agreements for Cambium and/or its agents. Cambium's and/or its agents intentional and willful acts to access and continue to access protected devices, Ubiquiti M-series devices and Ubiquiti websites used in interstate commerce and communications, to hack, copy, modify, remove, and make unauthorized use of Ubiquiti's firmware and M-series devices were all without authorization and in violation of the Computer Fraud and Abuse Act and the Illinois Computer Crime Prevention Law.

92. Cambium has provided information and firmware to facilitate users switching from signed AirOS firmware versions to the Hacked Firmware. *See* Postings on Cambium Community Forum, Exhibit K.

Cambium's False and Misleading Statements to Promote the Hacked Firmware

93. On and around November 30, 2016, Cambium made announcements on its website and released a webinar announcing the general availability of the Hacked Firmware as a replacement for Ubiquiti's native firmware. The lead speakers during the webinar were Defendants Sakid Ahmed and Dmitry Moiseev. The webinar directs viewers to the Cambium website to download the Hacked Firmware and provides instructions on how to navigate the Ubiquiti web user interfaces driven by Ubiquiti firmware on M-series Ubiquiti devices in order to replace the Ubiquiti firmware with Cambium's Hacked Firmware.

94. During the webinar Defendants Ahmed and Moiseev—Cambium representatives—directly targeted Ubiquiti customers—claiming that the Hacked Firmware would "support . . . XW-based Ubiquiti hardware (2013-current) [,and] XM-based Ubiquiti hardware (2013 and prior)" totaling 17 supported Ubiquiti models.

95. During the webinar, Defendants Ahmed and Moiseev touted that Cambium would "continue to develop ePMP Elevate" in order to provide "[s]upport for more Ubiquiti subscriber modules."

96. During the webinar, Defendants Ahmed and Moiseev also held a live demonstration providing step-by-step instructions to Ubiquiti customers on how to install the Hacked Firmware. Defendants Ahmed and Moiseev demonstrated in real time Cambium's improper hacking of the Ubiquiti product.

97. During the webinar, Cambium also showed its so-called "lab" wherein Cambium had on display the Ubiquiti M-series devices.

98. During the webinar, Defendants Ahmed and Moiseev answered nearly a dozen live questions from the audience specifically regarding Ubiquiti, including pertaining to the alteration of Ubiquiti hardware and the supposed ability to reverse changes made to the Ubiquiti firmware through installation of the Hacked Firmware.

99. During the webinar, Defendants Ahmed and Moiseev referred customers with warranty questions to the hardware manufacturers, which include Ubiquiti.

100. The webinar was conducted by Defendant Sakid Ahmed, Vice President of Engineering, along with Cambium employees involved in product design and development for the Hacked Firmware, including Dmitry Moiseev.

101. Defendants Ahmed and Moiseev's statements to the public implied that Ubiquiti endorsed the Hacked Firmware—a false and misleading fact.

102. Cambium and its representatives have made numerous misrepresentations during the webinar.

103. For instance, during the webinar, Cambium representatives stated that "Once you've uploaded ePMP Elevate . . . old manufacturers' firmware is not operating in any form." (Exhibit F), Webinar, at 49:56-50:03. This is false. Various parameters and other portions of the Ubiquiti M-series firmware code remain operative after the Hacked Firmware is installed.

104. There were also numerous false statements by omission made during the webinar.

105. For instance, Cambium never disclosed during the webinar or in any promotional materials for the Hacked Firmware the following critical facts:

- that use of the ePMP Elevate Software violates the terms of the Ubiquiti licensing agreements;
- that the changes made with the Cambium Firmware alters the device to be non-FCC compliant;
- that use of the ePMP Elevate Software violates the licensing terms, which also voids the warranty; and
- that use of the ePMP Elevate Software infringes Ubiquiti's intellectual property.

106. The individual Defendants routinely have publicly touted the purported benefits of the Hacked Firmware in an effort to attract Ubiquiti customers.

107. So too has Cambium Network's President and Chief Executive Officer, Atul Bhatnagar, who was quoted in a December 7, 2016 article and a November 30, 2016 blog post on the Cambium Website touting the purported benefits of the Hacking ePMP Elevate Firmware. *See* https://appdevelopermagazine.com/4690/2016/12/7/cambium-networks-jailbreaks-first-wireless-broadband-network/ (quoting Mr. Bhatnagar as emphasizing the fact that ePMP Elevate is compatible with various types of hardware: "ePMP Elevate is a software solution that is hardware agnostic[.]" "Network operators with radio hardware from one or multiple vendors can now operate one network with a common management system without replacing installed CPE hardware."); *see also* https://www.cambiumnetworks.com/blog/cambium-networks-announces-

new-epmp-elevate-platform-adding-new-capabilities-to-existing-wireless-broadband-networks/ (stating same).

108. Cambium promoted its Quick Start Guide during its November 30, 2016 webinar targeting Ubiquiti customers stating that Cambium "strongly recommends" viewers read the Quick Start Guide.

109. On information and belief, on or about November 30, 2016, Cambium released an ePMP Portfolio Overview, which identifies the Hacked Firmware as a product called "elevate" and uses the Ubiquiti trademark to refer to the devices on which Cambium's Hacked Firmware should be installed.

110. On information and belief, on or around November 30, 2016, Cambium released a Quick Start Guide instructing Ubiquiti customers on steps to download the Hacked Firmware from the Cambium website and install it through the web user interfaces driven by Ubiquiti firmware on M-series devices. The Quick Start Guide contained numerous material misrepresentations.

111. For instance, in its Quick Start Guide, Cambium stated that "[a]fter the upgrade, the ePMP Elevate subscribers retain only their configured IP Address and Device Name. All other parameters, including configured access points SSIDs, frequency configuration, VLAN, etc. may be configured over-the-air after upgrade to ePMP Elevate." ePMP Elevate Quick Start Guide v3.2 (Nov. 2016) (Ex. D) at pg. 5. This statement is literally false. Multiple Ubiquiti parameters are copied, maintained, and used by ePMP Elevate, the Hacked Firmware.

112. Cambium also made misleading and/or false representations in its Quick Start Guide regarding the impact of the Hacked Firmware on FCC Standards:

> FCC Standards:
>
> Caution! The user must ensure that deployed ePMP products operate in accordance to local regulatory limits. ePMP and ePMP

> Elevate-compatible devices may not share regulatory certifications in all regions.
>
> Some 3rd-party radio devices were originally FCC-certified and labeled to operate in the 5.8 GHz frequency range only. An ePMP Elevate upgrade enables 3rd-party radios to operate within the U-NII-1 through U-NII-4 frequency band range 5150 – 5980 MHz. To ensure FCC regulatory compliance for ePMP Elevate-upgraded radio devices:
>
> 1. A **new label must be applied** to the device with the updated FCC ID clearly visible. 3rd-party radio manufacturers support FCC label requests online (labels are shipped directly).
>
> 2. FCC-allowed transmit power in the 5.8 GHz band has been reduced with the latest regulatory guidelines. **ePMP Elevate adheres to these FCC power limits**, and an upgrade to ePMP Elevate software **may introduce a reduction of the device's operating transmit power to adhere to regulatory limits** (as a result of the ePMP access point's transmit power control mechanism).

ePMP Elevate Quick Start Guide v3.2 (Nov. 2016) (Ex. D) at pg. 2 (emphasis added).

113. These statements regarding compliance with FCC standards are false and/or misleading. The statement that "a reduction of the device's operating transmit power" may "adhere to regulatory limits" is false and/or misleading. These statements imply customers can comply with FCC standards using the Hacked Firmware on Ubiquiti's M-series devices, when this is inaccurate.

114. On information and belief, Cambium's promotion of its Hacked Firmware to Ubiquiti customers with Ubiquiti M-series devices contains false and misleading information about the nature of the Hacked Firmware and its impact after installation on Ubiquiti M-series devices.

115. On information and belief, Cambium promotes the Hacked Firmware, for example, by falsely stating that after installing the Hacked Firmware on a Ubiquiti M-series device the original firmware is no longer present or operating in any form.

116. On information and belief, Cambium also falsely promotes the Hacked Firmware to Ubiquiti customers by stating that the original device manufacturer provides a hardware warranty for the Ubiquiti M-series devices that have been hacked by the installation of Cambium's Hacked Firmware.

117. On information and belief, Cambium also falsely and misleadingly promotes the installation and use of Hacked Firmware to Ubiquiti customers with Ubiquiti M-series devices by stating that after hacking Ubiquiti M-series devices by installing Cambium's Hacked Firmware, that the hacker can ensure FCC compliance by having a third party manufacturer, who is not the source of the Hacked Firmware, generate and apply a new FCC label to the device.

118. On information and belief, Cambium's false and misleading promotion of the Hacked Firmware for use with Ubiquiti M-series devices was carried out in order to capitalize on the goodwill and brand recognition that Ubiquiti developed—through the investment of resources—in the marketplace Cambium directly targeted existing Ubiquiti customers in an effort to damage these customers' brand loyalty and recognition of the Ubiquiti name and high quality standards associated therewith.

119. On information and belief, Cambium's false and misleading promotion of the Hacked Firmware for use with Ubiquiti M-series devices was carried out for commercial reasons to sell new Cambium access points with which to interface a customer's installed base of Ubiquiti M-series products after those Ubiquiti M-series products have been hacked with the Hacked Firmware.

120. Cambium's website contains a "Community" forum where members of the public—including potential and current Ubiquiti customers—may post questions and comments.

121. During its November 30, 2016 webinar, Cambium encouraged listeners to use the Cambium Community forum, noting that its employees were "active" users of the Community forum.

122. Cambium personnel, posting under a Cambium account displaying the Cambium logo, frequently post on the Community.Cambiumnetworks.com website on various message boards.

123. Numerous of the message boards directly target Ubiquiti customers by referencing and commenting on Ubiquiti products.

124. On one message board thread entitled "Ubiquiti LB23 does not respond after installing Elevate", Luis—who is identified on the board as a Cambium Employee—responded to provide the customer advice on altering the Hacked Firmware. This demonstrates Cambium's direct efforts to target and interfere with Ubiquiti's relationships with its existing customers.

125. On one message board thread entitled "Turning UBNT to ePMP Subscribers" a Cambium employee, Defendant Sakid Ahmed—who was identified as the "Moderator" of the board—posted statements regarding Cambium's supposed power performance in order to encourage customer to install the Cambium Hacked Firmware.

126. In a post dated December 25, 2017, Defendant Dmitry—noted as an "occasional contributor"—posted on a message board instructing a user on how to use ePMP with Ubiquiti power supplies.

Cambium's Instructions to Ubiquiti Customers Induce Breach of the Ubiquiti Firmware License Agreements and Installation of the Hacked Firmware

127. Cambium's promotional videos and Quick Start Guide, among other forms of promotion, instruct Ubiquiti customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface. In some cases, Cambium instructs Ubiquiti

customers to download and install certain versions of Ubiquiti firmware prior to hacking a Ubiquiti M-series device by installing the Cambium Hacked Firmware.

128. The Ubiquiti M-series devices and the use of Ubiquiti firmware on the M-series devices are covered by Ubiquiti Firmware License Agreements.

129. In addition to Cambium's own breaches of Ubiquiti license Agreement by creating, using and distributing the Hacked Firmware, Cambium's instructions to Ubiquiti customers to hack the Ubiquiti M-series devices by installing the Hacked Firmware causes the customer to breach the Ubiquiti license agreements and is a further breach by Cambium.

130. Cambium's use of Ubiquiti's name and trademarks in promotion conveys that manufactures like Ubiquiti will honor hardware warranties after hacked firmware is installed by a customer. On information and belief, Cambium's statements that no firmware from Ubiquiti remains on the Ubiquiti device after installation, and that obtaining an FCC label from a third party manufacturer will ensure FCC compliance are all intentional, calculated, false and/or unauthorized statements by Cambium, who as a manufacturer of similar hardware, should know better. These calculated misrepresentations and unauthorized uses of Ubiquiti's name and trademarks deliberately aim to deceive and induce customers into hacking their existing installed base of Ubiquiti M-series devices with Cambium's Hacked Firmware for the purpose of selling more Cambium access points and hardware and migrating Ubiquiti customers to Cambium hardware.

The Hacking Enterprise and Its Racketeering Activity

131. Cambium sits at the helm of the Hacking Enterprise—an association-in-fact—consisting of Cambium, Cambium Networks, Sakid Ahmed, Dmitry Moiseev, and distributor Winncom. At all relevant times, the Hacking Enterprise constituted an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c).

132. At all relevant times, the Hacking Enterprise was engaged in interstate and international commerce and involved in activities affecting interstate and international commerce.

133. Although functioning as independent legal entities, Cambium, Cambium Networks, and Winncom joined together with Defendants Moiseev and Ahmed for the common purpose of ensuring financial gain for themselves through misleading Ubiquiti customers.

134. The purpose of the Hacking Enterprise was to carry out a scheme to obtain money by persuading Ubiquiti customers to leave for Cambium based on material misrepresentations and omission, and sell Cambium equipment by competing unfairly against Ubiquiti.

135. Cambium led this Hacking Enterprise, with Winncom and Defendants Moiseev and Ahmed assisting in attracting customers.

136. Cambium Networks helped fund the Hacking Enterprise, by providing monetary support to Cambium and having Cambium carry out all distribution to Winncom in the United States.

137. Defendants Ahmed and Moiseev marketed the Hacked Firmware to the public through promotional and instructional videos and, on information and belief, designed the Hacked Firmware.

138. The members of the Hacked Enterprise came together with the specific purpose of ensuring financial gain via misleading and inducing consumers to purchase and install the Hacked Firmware among other illicit business and profit gaining purposes. On information and belief, the members of the Hacking Enterprise exchanged numerous emails, phone calls, and communications to strategize regarding the launch of the Hacked Firmware and the best ways to attract Ubiquiti customers and ensure commercial success of the Hacked Firmware and attraction and long-term success of the Hacked Firmware.

139. Each member of the Hacking Enterprise was recruited by Cambium, and Cambium provided each member of the Hacking Enterprise financial incentives and/or direct financial benefit for participation in the Hacking Enterprise.

140. The Hacking Enterprise carried out its goal of ensuring financial gain by engaging in various acts of willful copyright infringement and mail and wire fraud to induce customers to partially remove Ubiquiti firmware by installing the Hacked Firmware, copying portions of the Ubiquiti firmware, and circumventing signed versions of Ubiquiti firmware without authorization to ensure that Ubiquiti M-series devices would no longer be compatible with a Ubiquiti network using Ubiquiti protocols and would instead be used with newly purchased Cambium networking equipment compatible with the Hacked Firmware.

141. The Hacking Enterprise trafficked in and made material misrepresentations and omissions regarding the Hacked Firmware specifically to defraud and induce end users and customers into breaching the Firmware License Agreement and to make changes to the Ubiquiti M-series device.

142. The scheme of the Hacking Enterprise has been going on since at least November 30, 2016, at which point in time Cambium, with the knowledge and encouragement of its parent corporation Cambium Networks and through its Vice President of Engineering Sakid Ahmed, as well as employee Dmitry Moiseev, in conjunction Winncom, began promoting the Hacked Firmware and offering it for sale on the internet to consumers.

143. The Hacking Enterprise carried out its goal of obtaining financial gain at the expense of customers and Ubiquiti through a pattern of racketeering activity.

144. First, the Hacking Enterprise members conspired together to concoct a scheme to mislead and induce customers to purchase and install the Hacked Firmware.

145. The scheme began with Cambium, working with the funding and encouragement of its parent Cambium Networks, entering into partnerships with Blip and Winncom to traffic in and promote the Hacked Firmware.

146. On information and belief, in exchange for offering positive statements regarding the use of the Hacked Firmware, Blip and Winncom were able to take advantage of Cambium's special discount offered to customers that "spread the word" regarding the Hacked Firmware.

147. The Hacking Enterprise accomplished its promotion of the Hacked Firmware and inducement of third-party purchases and installation in various ways.

148. For instance, Blip and the Hacking Enterprise conspired together to issue various public comments regarding purported benefits that Blip gained from installation of the Hacked Firmware.

149. On November 29, 2016, Cambium posted on its website a "Resource" which touted that Blip's use of the Hacked Firmware "dramatically improved performance."

150. Cambium also quoted from co-conspirator Blip's co-owner, Ian Ellison, in product release announcements that touted the benefits of the Hacked Firmware.

151. Cambium's citation to the benefits Blip purportedly incurred in using the Hacked Firmware was done in order to specifically target customers of Ubiquiti. And, on information and belief, the members of the Hacking Enterprise were all aware of Cambium's intent to advertise the purported benefits to Blip from using the Hacked Firmware.

152. Winncom posted on its website numerous advertisements touting the supposed benefits of the Hacked Firmware, including seven separate "EPMP Case Studies" describing the Hacked Firmware.

153. Winncom has held seminars for Cambium—in an effort to assist the Hacking Enterprise—at its goal of attracting customers. One such seminar, which included a product demonstration of the Hacked Firmware was held on October 7, 2017 at a WISPApalooza event.

154. Sakid Ahmed and Dmitry Moiseev attended the WISPApalooza event on behalf of Cambium in an effort to work with Winncom to spread false and misleading information regarding the Hacked Firmware and to lure away Ubiquiti customers.

155. Winncom also served as a "Connected Partner" for Cambium, receiving various benefits to "reward" Winncom for furthering the Hacking Enterprise's scheme.

156. On February 17, 2012, Cambium Networks posted on its website, a press release touting a new "Connected Partner Program" of which Winncom was a partner distributor.

157. Winncom's advertisement of the case studies discussing the Hacked Firmware was done in order to specifically target Ubiquiti customers and induce purchases and use of the Hacked Firmware.

158. The Hacking Enterprises' misleading advertisements and tutorials were provided to consumers to mislead them and induce them to install the Hacked Firmware on Ubiquiti M-series devices, notwithstanding that doing so would violate FCC rules and the Ubiquiti Firmware License Agreements, in order to damage Ubiquiti M-series devices and their licensed firmware by rendering them unable to communicate with other Ubiquiti devices using Ubiquiti protocols, and in order for Cambium to sell Cambium equipment with which the newly installed Hacked Firmware on Ubiquiti M-series devices is compatible.

159. Ubiquiti has been directly and proximately harmed by the Hacking Enterprises' false advertisements and statements because customers are misled and induced to violate Ubiquiti

Firmware License Agreements, Ubiquiti intellectual property rights and FCC rules by hacking the Ubiquiti product they purchased with the Hacked Firmware.

160. Although the full extent of wire and mail fraud carried out by the Hacking Enterprise in furtherance of their scheme to mislead consumers and sell the Hacked Firmware remains to be determined, the following are examples of fraudulent statements members of the Hacked Enterprise made using the U.S. Mail and/or interstate wires:

- The Cambium website's advertisement of a "Resource Guide" which discusses purported benefits Blip gained from installation of the Hacked Firmware, without disclosing the true nature of the Hacked Firmware.
- Cambium's running of "field experience" webinars wherein Cambium discussed Blip's experience using the Hacked Software, without disclosing the true nature of the Hacked Firmware.
- Cambium's launching and showing of various promotional videos on its website that discuss purported "benefits" of the Hacked Firmware and instruct Cambium Customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface, without disclosing the true nature of the Hacked Firmware.
- Cambium's issuance of a press release on November 30, 2016 touting the Hacked Firmware's benefit and Blip's experience, without disclosing the true nature of the Hacked Firmware.
- Cambium's November 30, 2016 webinar designed to target Ubiquiti customers and provide a step-by-step procedure for hacking the Ubiquiti M-series Firmware, which prominently featured Defendants Ahmed and Moiseev, which contained numerous material misrepresentations and omissions described in paragraphs 93-105, 108, *infra* and Exhibit F.
- Winncom's hosting of a ePMP course on October 7th-9th, 2017 at WSIPApalooza 2017—an event attended by Defendants Ahmed and Moiseev—wherein Winncom in connection with Cambium hosted a session regarding "hardware installation" which, upon information and belief, involved Winncom providing a how-to tutorial to WISPs who ultimately sold the Hacked Firmware to customers, without disclosing the true nature of the Hacked Firmware.
- Winncom's advertising campaign regarding it ePMP course at WISPApalooza in advance of the event in October 2017, which failed to disclose the true nature of the Hacked Firmware. *See* http://www.winncom.com/en/news/15358.

- Winncom's staging of a promotion via its website in the Russian language whereby licenses to Elevate were provided free of charge to potential customers to induce hacking of the Ubiquiti Firmware. Specifically, on a Winncom affiliate website, Winncom advertised that: Cambium Networks is launching a campaign to help owners of wireless networks built on Ubiquiti equipment upgrade their network by replacing old equipment with the base station of the ePMP1000 series or ePMP 2000. When purchasing new ePMP equipment, you get an Elevate license as a gift !!!" *See* http://winncom.ru/news/license-epmp-elevate (Exhibit L).

- Cambium's issuance of promotional videos and a Quick Start Guide, which instruct Cambium Customers to install the Hacked Firmware on their Ubiquiti M-series devices through the Ubiquiti M-series web interface, which failed to disclose the true nature of the Hacked Firmware. Upon information and belief, the promotional videos and Quick Start Guide were released via the Cambium website on or about November 30, 2016.

- Defendants Ahmed and Moiseev made numerous posts on Cambium's message boards disseminating false and misleading information regarding the Hacked Firmware and providing encouragement to customers installing the Hacked Firmware.

- With the knowledge and encouragement of Winncom, and Cambium Networks, Cambium hosted a video webinar featuring Defendants Ahmed and Moiseev in late 2016 wherein Cambium made false statements regarding the Hacked Firmware. These materially false statements and omissions are outlined in detail in paragraphs 93-105 of the instant Complaint.

- Cambium's publication of a Quick Start Guide containing materially false statements and omissions described herein at paragraphs 110-113 of the instant Complaint.

161. Each of these statements were made through the wires and/or the US mails with the intent to defraud and induce consumers to install the Hacked Firmware.

162. On information and belief, Cambium also used the U.S. Mail to send promotional advertisements which encouraged customers to use the Hacked Firmware on the Ubiquiti devices.

163. On information and belief, Cambium used the U.S. Mail to send invoices for the Hacked Firmware to customers throughout the United States, including in this District.

164. On information and belief, in furtherance of the Hacking Enterprise, the Hacking Enterprise members communicated with each other via e-mail communications and over the phone.

165. On information and belief, income in furtherance of the Hacking Enterprise's scheme as received via wires when customers paid on-line to purchase the Hacked Firmware.

166. The advertisements, promotions, and web videos on the Cambium site were broadcast to and viewed by consumers throughout the United States.

167. The advertisements on the Winncom website was viewed and transmitting via the wires to consumers throughout the United States.

FIRST CLAIM FOR RELIEF
(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)
(Asserted Against Cambium)

168. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

A. CFAA § 1030(a)(2)(C) Violations

169. Section 1030(a)(2)(C) of the CFAA prohibits a person from intentionally accessing a protected computer without or in excess of authorization and obtaining information from a protected computer.

170. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

171. Cambium has itself, and has aided and abetted others, to intentionally install the Hacked Firmware on Ubiquiti M-series devices in violation of multiple provisions of the Ubiquiti Firmware License Agreements, and by so doing makes unauthorized access to among other things, Ubiquiti M-series devices and licensed firmware including configuration and calibration

information on the Ubiquiti M-series devices (the protected computers) in order to damage and take control of the Ubiquiti M-series devices for Cambium's commercial purposes.

172. By virtue of this conduct, Cambium has violated and has conspired with others to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing Ubiquiti M-series devices, which consist of protected computers used for interstate commerce or communications, without authorization or by exceeding authorized access to the Ubiquiti M-series devices, and by accessing configuration and calibration information in order to take control of the Ubiquiti M-series devices for Cambium's commercial purposes.

173. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers of Ubiquiti M-series devices, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

174. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

175. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

176. Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(2)(C) of the CFAA in an amount to be determined at trial.

177. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, as provided by 18 U.S.C. § 1030(g).

B. CFAA § 1030(a)(4) Violations

178. Section 1030(a)(4) of the CFAA prohibits a person from knowingly, and with intent to defraud, accessing a protected computer without authorization or in excess of authorized access and by means of such conduct furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

179. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

180. Cambium developed the Hacked Firmware intentionally and to perform hacks of Ubiquiti M-series devices that violate the Ubiquiti Firmware License Agreements in multiple ways, including removing copyrighted portions and copying copyrighted portions all during unauthorized access and installation of the Hacked Firmware on a protected computer, the Ubiquiti M-series device.

181. Cambium itself and by conspiring with others has intentionally defrauded Ubiquiti customers, including with misrepresentations by Cambium as to the nature of the Hacked Firmware, into breaching the Ubiquiti Firmware License Agreements and hacking their Ubiquiti M-series devices in furtherance of Cambium's profit making scheme.

182. Cambium's above described conduct has resulted in loss and damage to Ubiquiti's reputation and by having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers of Ubiquiti M-series devices, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols, all of which greatly exceeds $5,000.

183. Indeed, on information and belief, the Hacked Firmware has been installed on hundreds of Ubiquiti M-series devices in the United States alone and Cambium itself charges an annual "license" fee of $35 per year for each installation of Hacked Firmware.

184. The configuration information and binary data obtained by Cambium from each unauthorized access to a Ubiquiti M-series device, and the impairment of the Ubiquiti firmware on those devices which render the M-series devices inoperable with other Ubiquiti devices using Ubiquiti protocols, is a scheme to defraud Ubiquiti and its customers that consists of more than the mere use of Ubiquiti M-series devices.

185. By its above described conduct, Cambium has violated § 1030(a)(4) of the CFAA, by knowingly and with intent to defraud, accessing Ubiquiti M-series devices, which consist of protected computers used for interstate commerce or communications, without authorization, or by exceeding their authorized access, and by means of such access furthering the intended fraud and obtaining configuration information and binary data necessary to operate each M-series device.

186. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware which underlies its Firmware License Agreements with customers impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

187. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

188. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct

189. Ubiquiti is entitled to damages for Cambium's violation of § 1030(a)(4) of the CFAA in an amount to be determined at trial.

190. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

C. CFAA § 1030(a)(5)(A) Violations

191. Section 1030(a)(5)(A) of the CFAA prohibits knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer.

192. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

193. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti firmware, which results in the Ubiquiti M-series devices being impaired and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

194. Cambium's Hacked Firmware directly and intentionally damages Ubiquiti and the Ubiquiti M-series devices. It alters the code on these devices and changes the composition of these devices in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

195. By its above described conduct, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), by knowingly causing the transmission of a program,

information, code or command, including causing the transmission of the Hacked Firmware, and as a result of such conduct, intentionally causing damage without authorization to a protected computer.

196. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

197. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

198. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

199. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(A) of the CFAA in an amount to be determined at trial.

200. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, and other equitable relief, as provided by 18 U.S.C. § 1030(g).

D. CFAA § 1030(a)(5)(B) Violations

201. Section 1030(a)(5)(B) of the CFAA prohibits a person from intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage.

202. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

203. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

204. Cambium's conduct is intentional, and its Hacked Firmware recklessly, and with full knowledge of Cambium, causes the damage to the Ubiquiti M-series devices described above in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

205. Cambium intentionally ignores the restrictions set forth in the Ubiquiti Firmware Licensing Agreements with malice and disregard, demonstrating its reckless behavior in transmitting and aiding and abetting third parties, including Ubiquiti's customers, in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to License Agreements.

206. Thus, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B), by intentionally accessing one or more M-series devices, which consist of protected computers, without authorization, and as a result of such conduct, recklessly causing damage.

207. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

208. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

209. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

210. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(B) of the CFAA in an amount to be determined at trial.

211. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

E. CFAA § 1030(a)(5)(C) Violations

212. Section 1030(a)(5)(C) of the CFAA prohibits a person from intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage and loss.

213. Ubiquiti's M-series devices are protected computers within the meaning of the CFAA because the M-series devices are used in and affect interstate commerce.

214. Cambium transmits and aids and abets third parties, including Ubiquiti's customers in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices including the removal of large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired and altered and no longer able to connect to other

Ubiquiti devices using Ubiquiti's wireless protocols. The code and information transmitted cause the unauthorized access and the damage to Ubiquiti and the Ubiquiti M-series devices.

215. Cambium intentionally developed the Hacked Firmware to directly damage Ubiquiti and the Ubiquiti M-series devices for commercial advantage. It removes and alters firmware code on these devices and changes the composition of these devices in direct violation of multiple provisions of the governing Ubiquiti Firmware Licensing Agreements.

216. Thus, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(C), by intentionally accessing one or more M-series devices, which consist of protected computers, and, as a result of the intentional access causing the damage and loss described herein.

217. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

218. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

219. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

220. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(5)(C) of the CFAA in an amount to be determined at trial.

221. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries,

entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

F. CFAA § 1030(a)(6)(A) Violations

222. Section 1030(a)(6)(A) of the CFAA prohibits a person from knowingly and with intent to defraud trafficking in any password or similar information through which a protected computer may be accessed without authorization, if such trafficking affects interstate or foreign commerce.

223. Cambium traffics in—sells and transports to customers and third-party sellers—the Hacked Firmware and additional programs, videos and guides instructing third parties how to hack and gain unauthorized access to Ubiquiti M-series devices.

224. Through the Hacked Firmware and additional materials, consumers learn how and are able to hack and gain unauthorized access to Ubiquiti's M-series Devices.

225. The Hacked Firmware and alteration of the M-series Devices caused by installation of the Hacked Firmware, which itself facilitates unauthorized access, affects interstate commerce, as the Hacked Firmware is being distributed by Cambium and used throughout the United States and the world.

226. By the above described conduct, Cambium has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(6)(A), by knowingly and with intent to defraud trafficking in information by distributing Hacked Firmware and additional programs, videos and guides instructing third parties how to hack and gain unauthorized access to Ubiquiti M-series devices, which trafficking and access has affected and continues to affect interstate commerce and communications and foreign commerce.

227. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware, which underlies its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

228. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

229. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

230. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(a)(6)(A) of the CFAA.

231. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief, as provided by 18 U.S.C. § 1030(g).

G. CFAA § 1030(b)Violations

232. Section 1030(b) of the CFAA prohibits a person from conspiring to violate any other subsection of the CFAA.

233. Cambium has violated the CFAA by conspiring to commit the 18 U.S.C. § 1030(a) offenses listed above.

234. Cambium has conspired with Ubiquiti licensees of M-series device firmware to intentionally make unauthorized access by installing the Hacked Firmware, and other third parties, including Blip, who traffic in the Hacked Firmware, related software, guides and videos for

Ubiquiti M-series devices and directly or indirectly facilitate unauthorized access to the Ubiquiti M-series devices and installation of the Hacked Firmware on Ubiquiti M-series devices.

235. Ubiquiti has sustained damage and loss by, *inter alia*, having the Ubiquiti Firmware which underlies its Firmware License Agreements with customers impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

236. Cambium's Hacked Firmware has been provided by Cambium and third parties authorized by Cambium to well in excess of ten (10) Ubiquiti M-series devices, which are protected computers.

237. Ubiquiti has spent in excess of $100,000 investigating the nature of the Hacked Firmware and the damage it causes to Ubiquiti Firmware on Ubiquiti M-series devices resulting from Cambium's wrongful conduct.

238. Accordingly, Ubiquiti is entitled to damages for Cambium's violation of Section 1030(b) of the CFAA.

239. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, and other equitable relief, as provided by 18 U.S.C. § 1030(g).

H. Allegations Applicable to All CFAA Violations Asserted Herein

240. Ubiquiti has been informed and believes and thereon alleges that the actions of Cambium are knowing, deliberate, willful and in utter disregard of Ubiquiti's rights under the CFAA.

241. Ubiquiti has standing to bring the Computer Fraud and Abuse Act claims set forth above, and is entitled to remedies at law and equity pursuant to 18 U.S.C. § 1030(g) because

Cambium's conduct has caused a loss to Ubiquiti during any one (1) year period aggregating far more than $5,000 in value as specified in 18 U.S.C. § 1030(c)(4)(A)(i)(I).

242. Ubiquiti has suffered loss and has spent in excess of $100,000 investigating the Hacked Firmware in response to learning of Cambium's promotion and distribution of its Hacked Firmware to Ubiquiti M-series device customers in order to determine the nature of the Hacked Firmware and determine its response to Cambium's unauthorized access and trafficking.

243. In addition to the loss and damage to Ubiquiti, Cambium's Hacked Firmware changes the radio characteristics of the Ubiquiti M-series devices, and the Hacked Firmware exceeds radio restrictions in place on the M-series devices and that form the basis of Ubiquiti's FCC equipment authorization for the M-series devices. As modified with the Hacked Firmware, the M-series devices violate FCC rules and may constitute a threat to public safety.

SECOND CLAIM FOR RELIEF
(Violations of §§ 1201(a)(1), 1201(a)(2) and
1202(b) of the Digital Millennium Copyright Act)
(Asserted against Cambium)

244. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

A. DMCA § 1201(a)(1) Violations

245. Section 1201(a)(1) of the DMCA provides that no person shall circumvent a technological measure that effectively controls access to a work protected under this title.

246. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

247. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of

Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

248. Cambium, individually and acting in concert and with third parties, has violated Ubiquiti's rights under 17 U.S.C. § 1201(a)(1) by directly circumventing access control measures that effectively control the ability to update or alter the firmware on Ubiquiti M-series devices by using the Hacked Firmware, which passes through Ubiquiti's access control measures for detecting unauthorized firmware, and allows the Hacked Firmware to install on Ubiquiti M-series devices and thereafter make unauthorized access and use of portions of Ubiquiti's copyrighted Firmware to take control of Ubiquiti M-series devices. The Hacked Firmware after installation disables Ubiquiti's access control measures.

249. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1201.

250. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

251. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

252. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

253. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law. Pursuant to 17 U.S.C. § 1203, Ubiquiti is also entitled to an award of attorneys' fees and costs.

B. DMCA § 1201(a)(2) Violations

254. Section 1201(a)(2) of the DMCA provides that no person shall traffic in any technology, product, service, device, component, or part thereof, that, among other things, is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title.

255. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

256. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

257. Cambium, individually and collectively, have directly, or acting in concert with a third party, violated Ubiquiti's rights under 17 U.S.C. § 1201(a)(2) by offering to the public, services and the Hacked Firmware to circumvent Ubiquiti's technological measures.

258. Such services include in-person educational seminars demonstrating hacking Ubiquiti M-series devices with Hacked Firmware to circumvent Ubiquiti's technological measures; disseminating quick start guides and on-line videos demonstrating how to circumvent technological measures on Ubiquiti M-series devices and install the Hacked Firmware; and disseminating instructions on how to defeat Ubiquiti's signature protected firmware on Ubiquiti Firmware versions 5.6.15 and later on Cambium's community website

community.cambiumnetworks.com (*See* https://community.cambiumnetworks.com/t5/ePMP-Elevate/Issues-elevating-Ubiquiti-devices-with-firmware-higher-than-5-6/td-p/78837).

259. Cambium traffics in such services and the Hacked Firmware, which are used to disable Ubiquiti's technological measures and make Ubiquiti M-series devices and Ubiquiti Firmware that remains on the Ubiquiti M-series devices available for unauthorized access, copying and use thereafter.

260. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1201.

261. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

262. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each violation of the DMCA.

263. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

264. Cambium' conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

C. DMCA § 1202(b) Violations

265. Section 1202(b) of the DMCA provides, among other things, that no person shall, without authorization of the copyright owner or the law intentionally remove or alter any copyright management information, or distribute copyright management information knowing that the copyright management information has been removed or altered without authority, knowing or

having reasonable grounds to know that it will induce, enable, facilitate, or conceal an infringement.

266. Ubiquiti's Firmware for its M-series products is subject to protection under the copyright laws of the United States.

267. Access to Ubiquiti's Firmware is subject to the Firmware License Agreement and is controlled by technological measures, namely signature protected firmware in the case of Ubiquiti Firmware versions 5.6.15 and later and software for detecting unauthorized firmware for Ubiquiti Firmware versions 5.6.14 and lower.

268. Ubiquiti's Firmware also includes user interface software that allows users to interface with Ubiquiti M-series devices and allows users to upload new firmware to Ubiquiti M-series devices. The user interface software within the Ubiquiti Firmware includes copyright management information that is presented to the user on each page of the user interface that identifies Ubiquiti as the copyright owner of the Ubiquiti Firmware for each M-series device.

269. Cambium, individually and collectively, have directly, or acting in concert with a third party, violated Ubiquiti's rights under 17 U.S.C. § 1202(b) by distributing Hacked Firmware directly and through distributors to Ubiquiti customers that circumvents Ubiquiti's technological measures, removes Ubiquiti's user interface software including its copyright management information, and replaces the copyright management information with a new statement that Cambium is the copyright owner.

270. Cambium's conduct has been willful. Despite the fact that Ubiquiti firmware remains on the Ubiquiti M-series device even after it is hacked with the Hacked Firmware by Defendants or a Ubiquiti customer at the urging of Cambium, Cambium has removed the Ubiquiti copyright management information in order to conceal Cambium's infringement of Ubiquiti's

copyrights in the Ubiquiti Firmware, knowing that this will induce and/or facilitate infringement of the Ubiquiti Firmware as the user interacts with the Hacked Firmware on hacked Ubiquiti M-series devices.

271. The conduct described above has cost Ubiquiti an amount to be determined at trial and constitutes a violation of 17 U.S.C. § 1202.

272. The conduct described above was willful and undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices. An award of statutory damages is necessary to dissuade Defendants and others from the use of the Hacked Firmware.

273. Accordingly, pursuant to 17 U.S.C. § 1203, Ubiquiti is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

274. Ubiquiti is also entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

275. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

THIRD CLAIM FOR RELIEF
(Violation of the Illinois Computer Crime Prevention Law, 720 Il. C.S. 5/17-51)
(Asserted Against Cambium)

276. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

277. Ubiquiti's M-series devices are computers which operate using Ubiquiti Firmware licensed by Ubiquiti to M-series device customers.

278. Cambium transmits and aids and abets third parties, including Ubiquiti's customers, in the installation of the Hacked Firmware on Ubiquiti M-series devices in violation of the access restrictions pursuant to Ubiquiti Firmware License Agreements, causing damage to the Ubiquiti M-series devices and the licensed Ubiquiti Firmware, including destroying large portions of the Ubiquiti Firmware, which results in the Ubiquiti M-series devices being impaired, no longer compliant with FCC rules and regulations and no longer able to connect to other Ubiquiti devices using Ubiquiti's wireless protocols.

279. Cambium's conduct is intentional, and without permission of Ubiquiti, and its Hacked Firmware causes the damage to the Ubiquiti M-series devices and Ubiquiti Firmware described above in direct violation of the governing Ubiquiti Firmware Licensing Agreements.

280. Ubiquiti has sustained damage by, *inter alia*, having the Ubiquiti M-series devices and Firmware, which underlie its Firmware License Agreements with customers, impaired and altered and no longer compatible with other Ubiquiti devices using Ubiquiti's wireless protocols.

281. Unless restrained and enjoined, Cambium will continue to commit such acts. Ubiquiti's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Ubiquiti to remedies, including injunctive relief, or other equitable relief.

FOURTH CLAIM FOR RELIEF
(Willful violation of the Copyright Act, 17 U.S.C. §§ 101, *et seq.*)
(Asserted Against Cambium)

282. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

283. Ubiquiti owns copyrights in the Ubiquiti Firmware and has registered the copyrights. As the owner of the copyrights, Ubiquiti maintains exclusive rights to, *inter alia*,

distribute and reproduce the Ubiquiti Firmware. Ubiquiti licenses the Ubiquiti Firmware on a non-exclusive basis to its customers for use with Ubiquiti M-series devices.

284. Cambium has directly infringed and will continue to infringe Ubiquiti's copyrights in the Ubiquiti Firmware by violating the Ubiquiti Firmware License Agreement and making unauthorized copies and use of Ubiquiti Firmware for Ubiquiti M-series devices.

285. Cambium has directly infringed and will continue to infringe Ubiquiti's copyrights in the Ubiquiti Firmware by hacking into Ubiquiti M-series devices by loading the Hacked Firmware onto M-series devices and causing the Ubiquiti M-series devices to execute the Hacked Firmware. The Hacked Firmware destroys the integrity of the Ubiquiti Firmware, creates an unauthorized derivative work of the Ubiquiti firmware, and makes unauthorized copies of the Ubiquiti firmware, all in violation of the copyright act.

286. Such acts of direct infringement include Cambium's development of the Hacked Firmware, Cambium's demonstration of hacking a Ubiquiti M-series device in instructional videos posted on the Internet, and on information and belief Cambium's demonstration of the infringement by hacking Ubiquiti M-series devices in live classes.

287. Cambium has contributed to and induced the infringement of Ubiquiti's copyrights in the Ubiquiti firmware by third parties, including Cambium's distributors and Ubiquiti customers, by one or more of the following actions: making the Hacked Firmware available for download, marketing and promoting the Hacked Firmware to Ubiquiti's M-series device customers, selling and distributing "licenses" to use the Hacked Firmware on Ubiquiti M-series products, distributing a "Quick Start Guide" instructing Ubiquiti M-series device users how to hack their device with the Hacked Firmware, and providing online videos, customer support and

live demonstrations encouraging and teaching Ubiquiti customers how to hack Ubiquiti M-series devices with Hacked Firmware.

288. The infringing conduct described above has damaged Ubiquiti in an amount to be determined at trial and constitutes violations of 17 U.S.C. § 501. Ubiquiti is entitled to recover, under the Copyright Act, actual damages it has sustained and any gains, profits and advantages obtained by Defendants as a result of their acts of infringement alleged above.

289. The conduct described above was willful, was undertaken with knowledge of wrongdoing, and was undertaken with commercial motives to sell licenses to the Hacked Firmware and Cambium hardware to interface with hacked Ubiquiti M-series devices.

290. Ubiquiti has registered copyrights for the Ubiquiti Firmware that predate the course of Defendants' infringing conduct. Ubiquiti seeks a determination of statutory damages in the maximum amount of $150,000.00 per work infringed in view of the willful and commercially motivated infringement by Cambium pursuant to 17 U.S.C. § 504.

291. Under the Copyright Act, Ubiquiti is entitled to recover costs, including attorneys' fees pursuant to 17 U.S.C. § 505, for Defendants' acts of infringement.

292. Cambium's conduct, unless enjoined by the Court, will cause irreparable harm to Ubiquiti, which has no adequate remedy at law.

293. Cambium's Hacked Firmware, unless impounded and destroyed, will also continue to make unauthorized use of the Ubiquiti firmware in hacked Ubiquiti M-series devices and will cause continuing damage to Ubiquiti.

FIFTH CLAIM FOR RELIEF
(False Advertising under § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B))
(Asserted Against Cambium)

294. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

295. Cambium has disseminated through its promotional materials for the Hacked Firmware, including but not limited to guides and online instructional webinar videos, false and misleading statements concerning Ubiquiti, and the nature and propriety of the Hacked Firmware in violation of § 43(a) of the Lanham Act. Cambium's false and misleading statements include, but are not limited to, statements concerning the amount of firmware from Ubiquiti left on Ubiquiti M-series devices and its use after being hacked with Cambium's Hacked Firmware, statements that a hardware warranty may be available after Hacked Firmware is installed, and statements that FCC compliance on a Ubiquiti M-series device modified with the Hacked Firmware can be ensured by asking the third party manufacturer to apply a new FCC label. These statements constitute false and deceptive advertising and are likely to mislead, and/or have misled, consumers and distributors about the nature, characteristics and quality of the Hacked Firmware. Cambium's false and misleading statements are intended to conceal Cambium's copyright infringement, sell licenses to the Hacked Firmware and Cambium products to interface with hacked Ubiquiti M-series devices, and attack the reputation, goodwill and market position of Ubiquiti.

296. Cambium has willfully, knowingly, and intentionally made and continues to make false descriptions in advertising, and unless enjoined by this Court, will continue to deceive, mislead, and confuse consumers and distributors into believing that, among other things, Cambium's creation and dissemination of Hacked Firmware for Ubiquiti M-series devices is lawful, supported by warranty coverage from Ubiquiti, and yields hacked Ubiquiti M-series

devices that are FCC complaint. Cambium's false and deceptive advertising and promotion of its Hacked Firmware is intentionally and specifically targeted at Ubiquiti M-series devices as part of a deceptive sales strategy to migrate Ubiquiti customers away from Ubiquiti products to Cambium products with which the hacked Ubiquiti M-series devices are compatible.

297. As a direct and proximate cause of Cambium's unlawful acts and practices, including those set forth above, Cambium has caused, is causing, and unless enjoined by this Court, will continue to cause immediate and irreparable harm to Ubiquiti, for which there is no adequate remedy at law, and for which Ubiquiti is entitled to injunctive relief. Cambium's acts, as described herein, are, and unless enjoined, will continue to be, in violation of Section 43(a) of the Lanham Act.

298. As a direct and proximate cause of Cambium's unlawful acts and practices, including those set forth above, Cambium has caused, is causing, and unless enjoined by this Court, will continue to cause Ubiquiti to suffer damages to its business, reputation, and goodwill, and the loss of sales and profits Ubiquiti would have made but for Cambium's acts.

299. Cambium has acted in bad faith and has willfully engaged in false advertising with the intent to injure Ubiquiti and deceive the public. Thus, in addition to the injunctive relief and damages requested herein, Ubiquiti is entitled to costs and attorneys' fees pursuant to 25 U.S.C. § 1117(a).

SIXTH CLAIM FOR RELIEF
(Breach of Contract)
(Asserted Against Cambium)

300. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

301. Cambium has freely entered into Ubiquiti's Firmware License Agreements by using Ubiquiti M-series devices and downloading Ubiquiti firmware and a valid and binding contract has been formed between Cambium and Ubiquiti as set forth in the Ubiquiti Firmware License Agreements.

302. There was valuable consideration exchanged in connection with the Firmware License Agreements. Specifically, Cambium was granted a limited license to use the Ubiquiti Firmware on M-series devices in exchange for Cambium's agreement to comply with the terms of use.

303. The Firmware License Agreements expressly prohibited Cambium from "remov[ing] or alter[ing] any Ubiquiti copyright, trademark or other proprietary rights notices from the Software or Content" including the user interface of the Ubiquiti Firmware or any Ubiquiti Device. *See* Ex. B at 1, 2 and Ex. C at 3.

304. The Firmware License Agreements further provided that Cambium "may not and shall not permit others to," *inter alia*,

> c. copy the Ubiquiti Firmware (except as expressly permitted above), or copy the accompanying documentation;
>
> d. modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including without limitation any such mechanism used to restrict or control the functionality of the Ubiquiti Firmware, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Ubiquiti Firmware (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or
>
> e. distribute, rent, transfer or grant any rights in the Ubiquiti Firmware or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Ubiquiti.

> f. remove any Ubiquiti copyright notice or Ubiquiti branding from the Ubiquiti Firmware or modify any user interface of the Ubiquiti Firmware or Ubiquiti Device.

305. The Firmware License Agreements provided that Cambium not do the following:

> remove or alter any copyright, trademark or other proprietary rights notices from the Software or Content, or use them in contravention of any such applicable notices;
>
> reverse engineer, decompile, translate, disassemble or otherwise attempt to (i) derive the source code or the underlying ideas, algorithms, structure or organization of any Software (except that the foregoing limitation does not apply to the extent that such activities may not be prohibited under applicable law); or (ii) defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Software, including, without limitation, any such mechanism used to restrict or control the functionality of the Software;
>
> use the Software in violation of any third-party rights or any local, state, national or international law or regulation, including, without limitation, any local country regulations related to operation within legal frequency channels, output power and Dynamic Frequency Selection (DFS) requirements;

306. Cambium breached the foregoing provisions of the Firmware License Agreements by the conduct described herein.

307. Specifically, Cambium engaged in unauthorized copying and use of the proprietary features of the Ubiquiti Firmware.

308. Cambium's Elevate Firmware Update replaced numerous sections of the Ubiquiti Firmware and used the Ubiquiti Firmware code in the resulting Elevate Firmware Update.

309. Cambium also modified the Ubiquiti Firmware and attempted to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Ubiquiti Firmware, including mechanisms use to control the functioning of the Ubiquiti Firmware.

310. Cambium also reverse engineered the Ubiquiti Firmware in order to create the Cambium Elevate Firmware. The Cambium Elevate Firmware makes unauthorized copies and use of various components of the Ubiquiti Firmware.

311. Cambium's actions resulted in the unauthorized modification of the Ubiquiti Firmware.

312. Cambium's actions of illicit copying and modification of the Ubiquiti Firmware were in violation of, *inter alia*, the copyright laws of the United States.

313. Cambium's breaches of the End User Agreement are material and eviscerate the limited use that Ubiquiti granted.

314. Cambium's breaches have proximately and directly caused damage to Ubiquiti. Users no longer have functioning Ubiquiti Firmware on their devices after installation of the Cambium Hacked Firmware.

SEVENTH CLAIM FOR RELIEF
(Tortious Interference With Contract)
(Asserted Against Cambium)

315. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

316. The Firmware License Agreements are binding and enforceable contracts.

317. Cambium had actual knowledge of the Firmware License Agreements and freely entered into them by virtue of Cambium's use of Ubiquiti M-series devices and firmware as described above.

318. Cambium's false and misleading advertisement and promotion of the Hacked Firmware used to induce end users to install the Hacked Firmware on Ubiquiti M-series devices

constitute intentional acts taken with knowledge that users would be induced into violating the terms of their Firmware License Agreements with Ubiquiti.

319. Cambium configured the Hacked Firmware to make changes to the Ubiquiti Firmware knowing that these changes would breach the express terms of Ubiquiti's Firmware License Agreements with end users.

320. Cambium's interference with the Firmware License Agreements between Ubiquiti and end users has harmed Ubiquiti by having induced and continuing to induce end users to violate the terms of their Firmware License Agreements with Ubiquiti and causing damage to M-series devices rendering them no longer compatible with Ubiquiti protocols used to communicate with other Ubiquiti devices, causing, *inter alia*, lost sales, infringement and reputational harm.

EIGHTH CLAIM FOR RELIEF
(Unfair Competition)
(Asserted Against Cambium)

321. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

322. Ubiquiti has invested considerable money and time into developing the Ubiquiti Firmware.

323. Cambium has reverse engineered the Ubiquiti Firmware to reap the benefits of Ubiquiti's substantial investment of time and money and to free-ride on Ubiquiti's costly investment.

324. Cambium also unfairly benefits from Ubiquiti's investment into development of the Ubiquiti Firmware insofar as the Cambium Elevate Firmware makes use of and alters elements from the Ubiquiti Firmware.

325. Cambium, through its videos targeting Ubiquiti customers and posting on message boards targeting Ubiquiti customers, has propagated false and misleading promotional materials for the Hacked Firmware and maliciously interfered with Ubiquiti's customer relationships in an effort to mislead and induce those customers become customers of Cambium.

326. Cambium's reverse engineering and use of Ubiquiti's firmware in connection with the launch of the Cambium's Hacked Firmware for Ubiquiti M-series devices also constitutes unfair competition.

327. Cambium's Hacked Firmware is a competing product to Ubiquiti's firmware for M-series devices that is promoted with misleading statements and that after installation damages Ubiquiti firmware on M-series devices.

328. Cambium and Ubiquiti are competitors in wireless devices and in the dissemination of firmware for wireless devices.

329. Cambium's alteration of the Ubiquiti firmware damages and otherwise dilutes the quality of the Ubiquiti Firmware and harms Ubiquiti and its customers who purchased the Ubiquiti product.

330. Cambium's unfairly competitive behavior has proximately and directly caused damage to Ubiquiti.

NINTH CLAIM FOR RELIEF
(Intentional Interference with Prospective Economic Advantage)
(Asserted Against Cambium)

331. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

332. Ubiquiti had a reasonable opportunity to obtain business advantage from customers and prospective customers who would purchase and make use of the Ubiquiti firmware.

333. Cambium was aware of Ubiquiti's relationship with current customers and expectations of obtaining business from its existing and other customers.

334. Indeed, Cambium specifically advertised the Hacked Firmware using deceptive and misleading descriptions to Ubiquiti customers and prospective customers.

335. Cambium intentionally and unjustifiably interfered with Ubiquiti's relationships with current and prospective customers.

336. Cambium unjustifiably misled and induced customers of Ubiquiti to install the Hacked Firmware in violation of Ubiquiti Firmware License Agreements, altering the Ubiquiti firmware on Ubiquiti M-series devices so that customers of Ubiquiti could no longer use the hacked M-series devices to communicate with other Ubiquiti devices using Ubiquiti wireless protocols, but instead could communicate with Cambium products.

337. Cambium induced customers to terminate and not enter into certain business relationships with Ubiquiti for the sale of Ubiquiti devices to communicate with the installed base of hacked Ubiquiti M-series running the Hacked Firmware.

338. Ubiquiti has thus lost both current and prospective customers and sales as a result of Cambium's deceptive and misleading actions and has been damaged as a result.

TENTH CLAIM FOR RELIEF
(Infringement of Registered Trademarks, § 32 Lanham Act, 15 U.S.C. § 1114)
(Asserted Against Cambium)

339. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

340. Cambium, without authorization from Ubiquiti, is using in interstate commerce for the purpose of promoting the downloading and use of Cambium's Hacked Firmware on Ubiquiti's M-series devices, the following Ubiquiti registered trademarks: UBIQUITI®, NANOSTATION®,

NANOBEAM®, NANOBRIDGE®, ROCKET®, and POWERBEAM®, in violation of § 32 of the Lanham Act.

341. Cambium's conduct is likely to have caused and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

342. Cambium's conduct is willful and an intentional violation of Ubiquiti's rights under § 32 of the Lanham Act, 15 U.S.C. § 1114.

ELEVENTH CLAIM FOR RELIEF
(False Designation of Origin, § 43(a) Lanham Act, 15 U.S.C. § 1125(a)(1)(A))
(Asserted Against Cambium)

343. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

344. Cambium, without authorization from Ubiquiti, is using Ubiquiti trademarks, including UBIQUITI®, NANOSTATION®, NANOBEAM®, NANOBRIDGE®, ROCKET®, and POWERBEAM®, for the purpose of promoting the downloading and use of its Hacked Firmware on Ubiquiti's M-series devices, in violation of § 43(a) of the Lanham Act.

345. Cambium's conduct is likely to have caused and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

346. Cambium's conduct is willful and an intentional violation of Ubiquiti's rights under § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(A).

TWELFTH CLAIM FOR RELIEF
(Common Law Trademark Infringement)
(Asserted Against Cambium)

347. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

348. Cambium, without authorization from Ubiquiti, is using Ubiquiti trademarks, including UBIQUITI, NANOSTATION, NANOBEAM, NANOBRIDGE, ROCKET, and POWERBEAM, for the purpose of promoting the downloading and use of its Hacked Firmware on Ubiquiti's M-series devices, in violation of § 43(a) of the Lanham Act.

349. Cambium's conduct is likely to have cause and will continue to cause confusion, mistake and deception among consumers as to the source, origin, sponsorship or approval by Ubiquiti of Cambium's Hacked Firmware for Ubiquiti's M-series devices.

350. Cambium's conduct is willful and an intentional violation of Ubiquiti's common law trademark rights.

THIRTEENTH CLAIM FOR RELIEF
(Common Law Misappropriation)
(Asserted Against Cambium)

351. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

352. Ubiquiti invested considerable time and money into developing its Ubiquiti firmware, Ubiquiti M-series devices, and its brand recognition.

353. Cambium misappropriated the Ubiquiti firmware, by distributing Hacked Firmware that still uses Ubiquiti firmware, deceiving customers regarding the nature of the Hacked Firmware, and inducing such customers to alter the Ubiquiti firmware on Ubiquiti M-series

devices with the Hacked Firmware in violation of the Ubiquiti Firmware License Agreements at little or no cost to Cambium.

354. Cambium has also improperly traded and attempted to induce business for itself by misusing the Ubiquiti name deceiving customers regarding the nature of the Hacked Firmware to induce customers to hack Ubiquiti M-series devices and purchase and install Cambium products.

355. As a direct and proximate result of Cambium's misappropriation of Ubiquiti's firmware, Ubiquiti M-series devices, and its brand recognition, Cambium has obtained new customers and a free ride from the use of Ubiquiti's firmware because Cambium bore little or no expense in acquiring customers and inducing those customers to alter and continue to use portions of the Ubiquiti firmware.

356. As a direct and proximate result of Cambium's misappropriation of Ubiquiti's firmware, Ubiquiti M-series devices, and its brand recognition, Ubiquiti has suffered damages, including reputational harm, loss of business, and commercial damage in the marketplace.

FOURTEENTH CLAIM FOR RELIEF
(Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c))
(Asserted Against Cambium)

357. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

358. Cambium, Cambium Networks, Winncom, Dmitry Moiseev, and Sakid Ahmed comprise the Hacking Enterprise. The Hacking Enterprise is an association-in-fact enterprise engaged in activities that affect interstate commerce.

359. Cambium oversees the Hacking Enterprise running its day-to-day operations, with Winncom serving Cambium's needs within the Hacking Enterprise.

360. Winncom reports to Cambium regarding its distribution and sales.

361. Cambium, in turn, keeps Cambium Networks apprised of the Hacking Enterprises' activities, profits, and distributions thereof.

362. Cambium agreed to and did conduct and participate in the conduct of the Hacking Enterprise's affairs through a pattern of racketeering activity and for the unlawful purpose of intentionally defrauding consumers into installing the Hacked Firmware, which in turn ensured financial gains for the Hacking Enterprise members above and beyond those which the members would have received had then been engaging solely in lawful activities.

363. To the extent known at this time and to be further developed through discovery of information exclusively within the possession, custody, control and knowledge of the Hacking Enterprise members, that pattern includes related acts of mail fraud and wire fraud, including, but not limited to the activities described in paragraphs 93-105, 110-126, 160, *supra*.

364. Cambium was involved in each of these racketeering acts, specifically orchestrating and arranging for the racketeering acts to occur through the Hacking Enterprise.

365. The acts set forth above, which happened over a period of years, constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

366. Because the Hacking Enterprise directly targeted Ubiquiti customers, Ubiquiti has lost customers as a result of the Hacking Enterprises' activities.

367. Given false and misleading statements and material omissions made by the members of the Hacking Enterprise through the wires and mail, Ubiquiti has lost consumer good will in the market place and its brand reputation has been harmed.

368. As a direct and proximate result of Cambium's racketeering activities and violations of 18 U.S.C. § 1962(c), Ubiquiti has been injured in its business and property in that:

Ubiquiti has lost customers and customers were induced to breach the terms of the Ubiquiti's Firmware Licensing Agreements, Ubiquiti's M-series devices and licensed firmware have been damaged by eliminating their compatibility with other Ubiquiti networking devices using Ubiquiti protocols, and Ubiquiti's licensed intellectual property rights have been violated, in each case through installation of the Hacked Firmware.

369. Thus, Ubiquiti prays that the Court compensate Ubiquiti for Cambium's racketeering activities and grant Ubiquiti legal relief to remedy Cambium's RICO violations.

370. As a result of Cambium's RICO violations, Ubiquiti has lost sales and prospective sales to consumers, in an amount to be determined at trial. Specifically, customers of Ubiquiti have—at the direction and bequest of Cambium and after hearing Cambium's false and inaccurate statements—installed the Hacked Firmware altering their Ubiquiti devices rendering them unable able to communicate with other Ubiquiti products using Ubiquiti protocols.

371. Cambium should be ordered to pay to Ubiquiti damages for Cambium's RICO violations which have resulted in the concrete financial losses outlined herein.

372. Ubiquiti is entitled to treble damages for the RICO violations alleged herein

FIFTEENTH CLAIM FOR RELIEF
(Violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(d))
(Asserted Against Cambium Networks, Blip, Winncom, Sakid Ahmed, and Dmitry Moiseev)

373. Ubiquiti incorporates by reference each of the foregoing paragraphs as if set forth fully herein.

374. In commission of the racketeering acts set forth herein, each member of the Hacking Enterprise and co-conspirator Blip conspired to violate the RICO statute in violation of 18 U.S.C. § 1962(d).

375. Specifically, the Hacking Enterprise members and co-conspirator Blip worked together to ensure financial gain at the expense of Ubiquiti's copyrights, trademarks, and customer base.

376. The members of the Hacking Enterprise worked together to exceed the permissible and ordinary scope of a manufacturer-distributor relationship. So too did co-conspirator Blip work with Cambium to exceed the ordinary scope of a manufacturer-distributor relationship.

377. The members of the Hacking Enterprise conspired together to promote false advertisement to customers through webinars and in person demonstrations involved the Hacked Firmware.

378. Each of the members of the Hacking Enterprise as well as co-conspirator Blip were aware of the fraudulent nature and scope of the Hacking Enterprise and agreed to assist the Hacking Enterprise in carrying out its fraudulent acts.

379. Each of the members of the Hacking Enterprise agreed to the commission of, or participate in, at least two of the racketeering acts described herein. So too did Blip.

380. Indeed, each of the members of the Hacking Enterprise was aware of the Hacking Enterprise and received direct personal financial gain from the activities of the Hacking Enterprise. Likewise, Blip received direct financial benefit as a result of the Hacking Enterprise's activities.

381. Each of the members of the Hacking Enterprise and co-conspirator Blip intended to and in fact did further the purposes of the Hacking Enterprise.

382. Each of the members of the Hacking Enterprise and co-conspirator Blip engaged in the RICO conspiracy in order to further their own personal interests and ensure financial health for themselves individually.

383. Each of the members of the Hacking Enterprise and co-conspirator Blip wanted to harm Ubiquiti's goodwill and customer standing in the market place.

384. Each of the members of the Hacking Enterprise was aware of Cambium's control and worked together to further that control. Blip likewise aided Cambium in its control of the Hacking Enterprise and profit seeking motive.

385. Cambium took the control of the Enterprise.

386. Cambium Networks placed Cambium at the helm and allowed Cambium to run the U.S. sales and operations of the Hacked Firmware.

387. Dmitry Moiseev and Sakid Ahmed advertised the Hacked firmware, monitored web boards pertaining to the Hacked Firmware, and answered individual questions from users regarding the Hacked Firmware.

388. Blip and Winncom conspired with Cambium to ensure Cambium's position of control in the Hacking Enterprise and supported Cambium's efforts to market the Hacked Firmware.

389. Cambium Networks provided financial support to Cambium to ensure its position as the leader of the Hacking Enterprise and also authorized discounts and personal financial gains for Blip and Winncom.

390. The members of the Hacking Enterprise knew that their actions were part of a pattern of racketeering activity and agreed to commit their actions in furtherance of the scheme described herein. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

391. Blip likewise worked with Cambium to ensure Cambium's role as the lead of the Hacking Enterprise, and knew that Cambium was carrying out a pattern of racketeering activity

along with various other members of the Hacking Enterprise and agreed to have Cambium commit its racketeering activities along with co-conspirators in furtherance of the scheme described herein. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

392. Each of the members of the Hacking Enterprise and co-conspirator Blip were aware that Cambium was directly targeting Ubiquiti customers and making misleading claims implying that the Hacked Firmware was appropriately used with Ubiquiti products.

393. The Hacking Enterprise is an enterprise engaged in and whose activities affect interstate commerce.

394. As a direct and proximate result of the Hacking Enterprise's conspiracy, conspiracy with Blip, and RICO violations flowing therefrom, Ubiquiti has been injured in its business and property in that Ubiquiti has lost customers, had its copyrights and trademarks violated by the Hacking Enterprise, and had its M-series devices converted to ones that are no longer FCC complaint and not compatible with Ubiquiti protocols used to communicate with other products sold by Ubiquiti.

395. Thus, Ubiquiti prays that the Court remedy the co-conspirators racketeering activities and grant Ubiquiti legal relief.

396. As a result of the co-conspirators' RICO violations, Ubiquiti has lost sales and prospective sales to consumers, in an amount to be determined at trial. Specifically, customers of Ubiquiti have—at the direction and bequest of Cambium and after hearing Cambium's false and inaccurate statements—installed the Hacked Firmware converting their Ubiquiti devices to ones no longer compliant with FCC rules and not compatible with Ubiquiti protocols used to communicate with other products sold by Ubiquiti.

397. Ubiquiti is entitled to damages for the Hacking Enterprise's RICO violations, carried out with the knowing assistance of co-conspirator Blip, which have resulted in the concrete financial losses outlined herein in the form of lost profits and customers.

398. Ubiquiti is entitled to treble damages for the RICO violations alleged herein.

RELIEF REQUESTED

WHEREFORE, Ubiquiti Networks, Inc. requests judgment against Defendants and seeks relief, as follows:

A. That judgment be entered for Ubiquiti and against Defendants on all Counts;

B. That this Court find that Cambium violated the Computer Fraud and Abuse Act;

C. That this Court find that Cambium has willfully engaged in false advertising in the promotion of its Hacked Firmware for Ubiquiti M-series devices;

D. That this Court find that Cambium breached its contract with Ubiquiti by violating the Ubiquiti Firmware License Agreements associated with the Ubiquiti Firmware and Ubiquiti M-series devices;

E. That Cambium, its officers, directors, agents, employees, affiliates, subsidiaries, and all other persons acting in concert with them, be temporarily, preliminarily, and permanently enjoined from directly or indirectly creating, distributing or promoting Hacked Firmware.

F. That Cambium be required to account for all gains, profits, and advantages derived from their acts of hacking, false advertising, and infringement and for their other violations of law;

G. That Ubiquiti be awarded its actual damages and any profits attributable to Defendants' causing damage and loss to Ubiquiti by virtue of its hacking and distribution of Hacked Firmware targeting Ubiquiti M-series devices to Ubiquiti's customers, false advertising directed to Ubiquiti's customers, tortious interference and unfair competition directed towards

Ubiquiti's customers and other trademark infringement, copyright infringement and violations of state and federal law.

H. That Defendants be required to deliver for impounding during the pendency of this action, and for destruction, all copies, reproductions, or derivative works of Ubiquiti Firmware or Hacked Firmware in Cambium's possession, custody or control and other promotional material targeting Hacked Firmware for Ubiquiti products;

I. That Defendants be required to retrieve and destroy all copies of the Hacked Firmware provided to distributors, customers and other agents and cancel all "licenses" to the Hacked Firmware.

J. That Defendants be required to delete permanently from Defendants' computers and information technology systems all electronic copies of Ubiquiti Firmware and the Hacked Firmware;

K. That Defendants be required to delete permanently, from any website that they own or control, all copies or reproductions of the Hacked Firmware and related promotional materials;

L. The Court award actual, exemplary and treble damages for the RICO violations.

M. That Ubiquiti be awarded reasonable attorneys' fees and costs incurred in connection with this action, including, but not limited to, reasonable attorneys' fees and costs incurred in connection with Defendants' violation of the Computer Fraud and Abuse Act, the Illinois Computer Crime Prevention Law, the Lanham Act, the Copyright Act, and the RICO Act.

N. That a jury hear Ubiquiti's claims; and,

O. That this Court grant any such other and further relief as it deems just and proper.

Dated: August 7, 2018

Respectfully submitted,

MORGAN, LEWIS & BOCKIUS LLP

/s/ *Elizabeth B. Herrington*
Elizabeth B. Herrington (IL Bar No. 6244547)
77 West Wacker Drive
Chicago, IL 60601-5094
312.324.1000 (Telephone)
312.324.1001 (Facsimile)
beth.herrington@morganlewis.com

Robert C. Bertin
1111 Pennsylvania Avenue, NW
Washington, DC 20004-2541
202.739.3000 (Telephone)
202.739.3001 (Facsimile)
robert.bertin@morganlewis.com

Mark L. Krotoski
1400 Page Mill Road
Palo Alto, CA 94304-1124
650.843.4000 (Telephone)
650.843.4001 (Facsimile)
mark.krotoski@morganlewis.com

Amy M. Dudash
1701 Market Street
Philadelphia, PA 19103
215.963.5000 (Telephone)
215.963.5001 (Facsimile)
amy.dudash@morganlewis.com

Attorneys for Plaintiff Ubiquiti Networks, Inc.